
Informacijska tehnologija – Varnostne tehnike – Sistemi vodenja informacijske varnosti – Pregled in izrazje (ISO/IEC 27000:2018)

Information technology – Security techniques – Information security management systems – Overview and vocabulary (ISO/IEC 27000:2018)

Informationstechnik – Sicherheitsverfahren – Informationssicherheits-
Managementsysteme – Überblick und Terminologie (ISO/IEC 27000:2018)

Technologies de l'information – Techniques de sécurité – Systèmes de
management de la sécurité de l'information – Vue d'ensemble et vocabulaire
(ISO/IEC 27000:2018)

[SIST EN ISO/IEC 27000:2020](https://standards.iteh.ai/catalog/standards/sist/fb0bcd63-297a-4cdc-883a-a79589b56f25/sist-en-iso-iec-27000-2020)

<https://standards.iteh.ai/catalog/standards/sist/fb0bcd63-297a-4cdc-883a-a79589b56f25/sist-en-iso-iec-27000-2020>

ICS 01.040.35; 03.100.70; 35.030

Referenčna oznaka
SIST EN ISO/IEC 27000 : 2020 (sl)

Nadaljevanje na straneh II in III ter od 2 do 34

NACIONALNI UVOD

Standard SIST EN ISO/IEC 27000 (sl), Informacijska tehnologija – Varnostne tehnike – Sistemi vodenja informacijske varnosti – Pregled in izrazje (ISO/IEC 27000:2018), 2020, ima status slovenskega standarda in je enakovreden evropskemu standardu EN ISO/IEC 27000 (en, fr, de), Information technology – Security techniques – Information security management systems – Overview and vocabulary (ISO/IEC 27000:2018), 2020.

NACIONALNI PREDGOVOR

Besedilo standarda EN ISO/IEC 27000:2020 je pripravil združeni tehnični odbor Mednarodne organizacije za standardizacijo (ISO) in Mednarodne elektrotehniške komisije (IEC) ISO/IEC JTC 1 Informacijska tehnologija. Slovenski standard SIST EN ISO/IEC 27000:2020 je prevod angleškega besedila evropskega standarda EN ISO/IEC 27000:2020. V primeru spora glede besedila slovenskega prevoda v tem standardu je odločilen izvorni evropski standard v angleškem jeziku. Slovensko izdajo standarda je pripravil SIST/TC ITC Informacijska tehnologija.

Odločitev za privzem tega standarda je dne 18. 11. 2024 sprejel SIST/TC ITC Informacijska tehnologija.

OSNOVA ZA IZDAJO STANDARDARDA

- privzem standarda EN ISO/IEC 27000:2020

PREDHODNA IZDAJA

- SIST EN ISO/IEC 27000:2017, Informacijska tehnologija – Varnostne tehnike – Sistemi upravljanja informacijske varnosti – Pregled in izrazje (ISO/IEC 27000:2016)

OPOMBE

- Povsod, kjer se v besedilu standarda uporablja izraz "evropski standard", v SIST EN ISO/IEC 27000:2020 to pomeni "slovenski standard".
- Nacionalni uvod in nacionalni predgovor nista sestavni del standarda.
- V podtočki 5.4.10 (točke 5.4 Standardi, ki opisujejo splošne smernice) je v evropskem standardu naveden napačen naslov standarda ISO/IEC 27021. Pravi naslov je "Information technology – Security techniques – Competence requirements for information security management systems professionals".
- V podtočki 5.4.2 (točke 5.4 Standardi, ki opisujejo splošne smernice) ter poglavju Viri in literatura je v evropskem standardu naveden napačen naslov standarda ISO/IEC 27003. Pravi naslov je "Information technology – Security techniques – Information security management systems – Guidance".
- Ta nacionalni dokument je enakovreden EN ISO/IEC 27000:2020 in je objavljen z dovoljenjem

CEN-CENELEC
Upravni center
Rue de la Science 23
B-1040 Bruselj
Belgija

- This national document is identical with EN ISO 27000:2020 and is published with the permission of

CEN-CENELEC
Management Centre
Rue de la Science 23
B-1040 Brussels
Belgium

iTeh Standards
(<https://standards.iteh.ai>)
Document Preview

[SIST EN ISO/IEC 27000:2020](https://standards.iteh.ai/catalog/standards/sist/fb0bcd63-297a-4cdc-883a-a79589b56f25/sist-en-iso-iec-27000-2020)

<https://standards.iteh.ai/catalog/standards/sist/fb0bcd63-297a-4cdc-883a-a79589b56f25/sist-en-iso-iec-27000-2020>

iTeh Standards
(prazna stran)
(<https://standards.itih.ai>)
Document Preview

[SIST EN ISO/IEC 27000:2020](https://standards.itih.ai/catalog/standards/sist/fb0bcd63-297a-4cdc-883a-a79589b56f25/sist-en-iso-iec-27000-2020)

<https://standards.itih.ai/catalog/standards/sist/fb0bcd63-297a-4cdc-883a-a79589b56f25/sist-en-iso-iec-27000-2020>

Slovenska izdaja

**Informacijska tehnologija – Varnostne tehnike – Sistemi vodenja
informacijske varnosti – Pregled in izrazje
(ISO/IEC 27000:2018)**

Information technology – Security
techniques – Information security
management systems – Overview
and vocabulary (ISO/IEC
27000:2018)

Technologies de l'information –
Techniques de sécurité –
Systèmes de management de la
sécurité de l'information – Vue
d'ensemble et vocabulaire
(ISO/IEC 27000:2018)

Informationstechnik –
Sicherheitsverfahren –
Informationssicherheits-
Managementsysteme – Überblick
und Terminologie (ISO/IEC
27000:2018)

Ta evropski standard je CEN sprejel dne 20. oktobra 2019.

Člani CEN in CENELEC morajo izpolnjevati notranje predpise CEN/CENELEC, s katerimi je predpisano, da mora biti ta standard brez kakršnihkoli sprememb sprejet kot nacionalni standard. Seznami najnovjših izdaj teh nacionalnih standardov in njihovi bibliografski podatki so na zahtevo na voljo pri Upravnem centru CEN-CENELEC ali kateremkoli članu CEN in CENELEC.

Ta evropski standard obstaja v treh uradnih izdajah (angleški, francoski, nemški). Izdaje v drugih jezikih, ki jih člani CEN in CENELEC na lastno odgovornost prevedejo in izdajo ter prijavijo pri Upravnem centru CEN-CENELEC, veljajo kot uradne izdaje.

Člani CEN in CENELEC so nacionalni organi za standarde in nacionalni elektrotehniški odbori Avstrije, Belgije, Bolgarije, Cipra, Češke republike, Danske, Estonije, Finske, Francije, Grčije, Hrvaške, Irske, Islandije, Italije, Latvije, Litve, Luksemburga, Madžarske, Malte, Nemčije, Nizozemske, Norveške, Poljske, Portugalske, Republike Severna Makedonija, Romunije, Slovaške, Slovenije, Srbije, Španije, Švedske, Švice, Turčije in Združenega kraljestva.

CEN-CENELEC

CEN-CENELEC Upravni center
Rue de la Science 23, B-1040 Bruselj

VSEBINA

Stran

Evropski predgovor.....3

iTeh Standards
(<https://standards.itih.ai>)
Document Preview

[SIST EN ISO/IEC 27000:2020](https://standards.itih.ai/catalog/standards/sist/fb0bcd63-297a-4cdc-883a-a79589b56f25/sist-en-iso-iec-27000-2020)

<https://standards.itih.ai/catalog/standards/sist/fb0bcd63-297a-4cdc-883a-a79589b56f25/sist-en-iso-iec-27000-2020>

Evropski predgovor

Besedilo standarda ISO/IEC 27000:2018 je pripravil tehnični odbor ISO/IEC JTC 1 "Informacijska tehnologija" Mednarodne organizacije za standardizacijo (ISO) in ga je kot EN ISO/IEC 27000:2020 sprejel tehnični odbor CEN/CLC/JTC 13 "Kibernetska varnost in varstvo podatkov", katerega sekretariat vodi DIN.

Ta evropski standard mora z objavo istovetnega besedila ali z razglasitvijo dobiti status nacionalnega standarda najpozneje do avgusta 2020, nacionalne standarde, ki so v nasprotju s tem standardom, pa je treba razveljaviti najpozneje do avgusta 2020.

Opozoriti je treba na možnost, da je lahko nekaj elementov tega dokumenta predmet patentnih pravic. CEN ni odgovoren za identificiranje katerekoli ali vseh takih patentnih pravic.

Ta dokument nadomešča EN ISO/IEC 27000:2017.

V skladu z notranjimi predpisi CEN-CENELEC morajo ta evropski standard obvezno uvesti nacionalne organizacije za standardizacijo naslednjih držav: Avstrije, Belgije, Bolgarije, Cipra, Češke republike, Danske, Estonije, Finske, Francije, Grčije, Hrvaške, Irske, Islandije, Italije, Latvije, Litve, Luksemburga, Madžarske, Malte, Nemčije, Nizozemske, Norveške, Poljske, Portugalske, Republike Severna Makedonija, Romunije, Slovaške, Slovenije, Srbije, Španije, Švedske, Švice, Turčije in Združenega kraljestva.

Razglasitvena objava

Besedilo standarda ISO/IEC 27000:2018 je CEN odobril kot EN ISO/IEC 27000:2020 brez sprememb.

(<https://standards.iteh.ai>)
Document Preview

[SIST EN ISO/IEC 27000:2020](https://standards.iteh.ai/catalog/standards/sist/fb0bcd63-297a-4cdc-883a-a79589b56f25/sist-en-iso-iec-27000-2020)

<https://standards.iteh.ai/catalog/standards/sist/fb0bcd63-297a-4cdc-883a-a79589b56f25/sist-en-iso-iec-27000-2020>

Vsebina	Stran
Predgovor k mednarodnemu standardu.....	6
Uvod.....	7
1 Področje uporabe.....	8
2 Zveze s standardi.....	8
3 Izrazi in definicije.....	8
4 Sistemi vodenja informacijske varnosti.....	18
4.1 Splošno.....	18
4.2 Kaj je sistem vodenja informacijske varnosti?.....	18
4.2.1 Pregled in načela.....	18
4.2.2 Informacija.....	19
4.2.3 Informacijska varnost.....	19
4.2.4 Vodenje.....	19
4.2.5 Sistem vodenja.....	20
4.3 Procesni pristop.....	20
4.4 Zakaj je sistem vodenja informacijske varnosti pomemben.....	20
4.5 Vzpostavljanje, spremljanje, vzdrževanje in izboljševanje sistema vodenja informacijske varnosti.....	21
4.5.1 Pregled.....	21
4.5.2 Prepoznavanje zahtev informacijske varnosti.....	21
4.5.3 Ocenjevanje tveganj informacijske varnosti.....	22
4.5.4 Obravnavanje tveganj informacijske varnosti.....	22
4.5.5 Izbiranje in izvajanje kontrol.....	22
4.5.6 Spremljanje, vzdrževanje in izboljševanje uspešnosti sistema vodenja informacijske varnosti.....	23
4.5.7 Nenehno izboljševanje.....	24
4.6 Ključni dejavniki uspeha sistema vodenja informacijske varnosti.....	24
4.7 Koristi skupine standardov za sistem vodenja informacijske varnosti.....	24
5 Skupina standardov za sistem vodenja informacijske varnosti.....	25
5.1 Splošne informacije.....	25
5.2 Standardi, ki opisujejo pregled in terminologijo: ISO/IEC 27000 (ta dokument).....	26
5.3 Standardi, ki določajo zahteve.....	26
5.3.1 ISO/IEC 27001.....	26
5.3.2 ISO/IEC 27006.....	27
5.3.3 ISO/IEC 27009.....	27
5.4 Standardi, ki opisujejo splošne smernice.....	27
5.4.1 ISO/IEC 27002.....	27
5.4.2 ISO/IEC 27003.....	28
5.4.3 ISO/IEC 27004.....	28
5.4.4 ISO/IEC 27005.....	28

5.4.5 ISO/IEC 27007	28
5.4.6 ISO/IEC TR 27008	28
5.4.7 ISO/IEC 27013	29
5.4.8 ISO/IEC 27014	29
5.4.9 ISO/IEC TR 27016	29
5.4.10 ISO/IEC 27021	30
5.5 Standardi, ki opisujejo smernice za določene sektorje.....	30
5.5.1 ISO/IEC 27010	30
5.5.2 ISO/IEC 27011	30
5.5.3 ISO/IEC 27017	31
5.5.4 ISO/IEC 27018	31
5.5.5 ISO/IEC 27019	31
5.5.6 ISO 27799	32
Viri in literatura.....	33

iTeh Standards
(<https://standards.itih.ai>)
Document Preview

[SIST EN ISO/IEC 27000:2020](#)

<https://standards.itih.ai/catalog/standards/sist/fb0bcd63-297a-4cdc-883a-a79589b56f25/sist-en-iso-iec-27000-2020>

Predgovor k mednarodnemu standardu

ISO (Mednarodna organizacija za standardizacijo) je svetovna zveza nacionalnih organov za standarde (članov ISO). Mednarodne standarde po navadi pripravljajo tehnični odbori ISO. Vsak član, ki želi delovati na določenem področju, za katero je bil ustanovljen tehnični odbor, ima pravico biti zastopan v tem odboru. Pri delu sodelujejo tudi mednarodne vladne in nevladne organizacije, povezane z ISO. V vseh zadevah, ki so povezane s standardizacijo na področju elektrotehnike, ISO tesno sodeluje z Mednarodno elektrotehniško komisijo (IEC).

Postopki, uporabljeni pri pripravi tega dokumenta, in predvideni postopki za njegovo vzdrževanje so opisani v 1. delu Direktiv ISO/IEC. Posebna pozornost naj se nameni različnim kriterijem odobritve, potrebnim za različne vrste dokumentov ISO. Ta dokument je bil zasnovan v skladu z uredniškimi pravili Direktiv ISO/IEC, 2. del (glej www.iso.org/directives).

Opozoriti je treba na možnost, da bi lahko bil kateri od elementov tega dokumenta predmet patentnih pravic. ISO ni odgovoren za identificiranje katerekoli ali vseh takih patentnih pravic. Podrobnosti o morebitnih patentnih pravicah, identificiranih med pripravo tega dokumenta, bodo navedene v uvodu in/ali na seznamu patentnih izjav, ki jih je prejela organizacija ISO (glej www.iso.org/patents).

Vsakršna trgovska imena, uporabljena v tem dokumentu, so informacije za uporabnike in ne pomenijo podpore blagovni znamki.

Za razlago prostovoljne narave standardov, pomena specifičnih pojmov in izrazov ISO, povezanih z ugotavljanjem skladnosti, ter informacij o tem, kako ISO upošteva načela Svetovne trgovske organizacije (WTO) v Tehničnih ovirah pri trgovanju (TBT), glej naslednjo povezavo: www.iso.org/iso/foreword.html.

Ta dokument je pripravil tehnični odbor ISO/IEC JTC 1 *Informacijska tehnologija*, pododbor SC 27 *Varnostne tehnike IT*.

Ta peta izdaja preklicuje in nadomešča četrto izdajo (ISO/IEC 27000:2016), ki je tehnično revidirana. Glavne spremembe glede na predhodno izdajo so naslednje:

- uvod je preoblikovan,
- nekateri izrazi in definicije so odstranjeni,
- [točka 3](#) je usklajena s strukturo visoke ravni standardov za sisteme vodenja (MSS),
- [točka 5](#) je posodobljena tako, da odraža spremembe v zadevnih standardih,
- dodatka A in B sta izbrisana.

Uvod

0.1 Pregled

Mednarodni standardi za sisteme vodenja zagotavljajo model kot zgled za vzpostavitev in upravljanje sistema vodenja. Ta model vključuje značilnosti, o katerih so si strokovnjaki na tem področju enotni, da gre za mednarodno stanje tehnike. V okviru ISO/IEC JTC 1/SC 27 deluje strokovni odbor, namenjen razvoju mednarodnih standardov za sisteme vodenja informacijske varnosti, sicer znanih kot skupina standardov za sistem vodenja informacijske varnosti (ISMS).

Z uporabo skupine standardov za sistem vodenja informacijske varnosti lahko organizacije razvijejo in uporabljajo okvir za upravljanje varnosti svojih informacijskih sredstev, vključno s finančnimi podatki, intelektualno lastnino in podatki o zaposlenih, ali informacij, ki so jim jih zaupali odjemalci ali tretje stranke. Ti standardi se lahko uporabljajo tudi za priprave na neodvisno ocenjevanje njihovega sistema vodenja informacijske varnosti, ki se uporablja za zaščito informacij.

0.2 Namen tega dokumenta

V skupini standardov za sistem vodenja informacijske varnosti so standardi, ki:

- a) opredeljujejo zahteve za sistem vodenja informacijske varnosti in za vse, ki certificirajo take sisteme;
- b) zagotavljajo neposredno podporo, podrobne napotke in/ali razlago za celoten proces vzpostavitve, izvajanja, vzdrževanja in izboljšanja sistema vodenja informacijske varnosti;
- c) obravnavajo področno specifične smernice za sistem vodenja informacijske varnosti; in
- d) obravnavajo ugotavljanje skladnosti sistema vodenja informacijske varnosti.

0.3 Vsebina tega dokumenta

V tem dokumentu so uporabljene naslednje glagolske oblike:

- "treba je" ali "mora" označuje zahtevo;
- "naj" označuje priporočilo;
- "sme" označuje dovoljenje;
- "lahko" označuje možnost ali sposobnost.

Informacije, označene kot "OPOMBA", so namenjene usmerjanju pri razumevanju ali pojasnjevanju pripadajoče zahteve. "OPOMBE" v točki 3 podajajo dodatne informacije, ki dopolnjujejo terminološke podatke in lahko vsebujejo določila v zvezi z uporabo izraza.